UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,509	03/28/2001	Mahfuzur Rahman	MATI-202US	4790

23122　　7590　　12/28/2005

RATNERPRESTIA
P O BOX 980
VALLEY FORGE, PA 19482-0980

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/819,509	RAHMAN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claim 6 has been amended.

2. Claims 21-22 have been added.

3. Claims 1-22 are pending.

Response to Arguments

4. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection, in view of Baird, III et al., (Pub No. 2004/0230807) and Epstein (Pub No. 2002/0124176).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1-13 and 15-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Baird, III et al. (Pub No. 2004/0230807).

Regarding claims 1 and 16, Baird III, et al. discloses a method for forming a strong password comprising the steps of:

obtaining biometric data from a user (See Page 4, Section 0029)

generating a one-time password for the user (See Page 4, Section 0029)

and combining the biometric data and the one-time password to form the strong password (See Page 4, Sections 0029 and 0033-0034)

Regarding claims 2 and 17, Baird III, et al. discloses the claimed limitation wherein comprising the step of encrypting the combined one-time password and biometric data using an encryption key to form the strong password (See Page 7, Section 0059)

Regarding claims 3 and 18, Baird III, et al. discloses a method and computer program for controlling access to secure data comprising the data from a user:

receiving a strong password including one-time password and biometric data (See Page 9, Section 0074)

separating the one-time password and the biometric data (See Page 9, Section 0075)

comparing the one-time password to a calculated one-time password to determine if the one-time password is valid (See Page 9, Section 0075)

determining a probability that the biometric data is from the user (See Page 9, Section 0076) encrypting the secure data using an encryption key to obtain encrypted data if the one-time password matches the calculated one-time password and the probability that the biometric data is from the user exceeds a predetermined threshold value (See Page 10, Section 0077)

combining the strong password, the encryption key and the encryption data (See Page 10, Section 0078)

and transmitting the combined strong password, encryption key and encrypted data to the user (See Page 10, Section 0079)

Regarding claims 4 and 19, Baird III, et al. discloses the claimed limitation wherein the step of encrypting the combined strong password and encryption key using a further encryption key (See Page 7, Section 0059)

Regarding claims 5 and 20, Baird III, et al. discloses the claimed limitation wherein the secure data includes items having respectively different security levels, and the step of encrypting the secure data aborts the method if either the one-time password does not match the calculated one-time password or the probability that the biometric data is from the user does not exceed the predetermined threshold value (See Page 1, Section 0006 and Page 6, Section 0035)

Regarding claim 6 Baird III, et al. discloses a system for implementing secure access to a remote computer system comprising:

at least one first computer securely coupled to the remote computer system (See Page 2, Section 0019) at least one second computer coupled to the at least one first computer and configured to obtain identifying information from a user (See Page 3, Section 0023)

wherein the second computer passes the identifying information to the first computer, the first computer passes the identifying information to the remote computer system and the remote computer system verifies the identifying information (See Pages 3-4, Section 0029)

Regarding claim 7, Baird III, et al. discloses the claimed limitation wherein the identifying information is a strong password including a one-time password and biometric information (See Page 7, Section 0055)

Regarding claim 8, Baird III, et al. discloses the claimed limitation wherein the identifying information is encrypted with an encryption key (See Page 6, Section 0035)

Regarding claim 9, Baird III, et al. discloses the claimed limitation wherein the second computer is securely connected to the first computer by means of a Secure Socket Layer connection (See Page 2, Section 0020)

Regarding claim 10, Baird III, et al. discloses the claimed limitation wherein the second computer includes a further Secure Socket Layer connection for receiving the identifying information from the user (See Page 7, Section 0052)

Regarding claim 11, Baird III, et al. discloses the claimed limitation wherein the remote computer includes firewall software through which the first computer is coupled to a remote computer (See Page 2, Section 0019 and Page 3, Section 0024)

Regarding claim 12, Baird III, et al. discloses a method of allowing access to secure data on a remote computer including the steps of:

receiving a request from a user to access the secure data at a first computer (See Page 9, Section 0074)

transferring the request to access the secure data from the first computer to the second computer (See Page 9, Section 0075)

transferring the request to access the secure data from the second computer to the remote computer (See Page 9, Section 0076)

authorizing access to the secure data at the remote computer (See Pages 9-10, Sections 0076-0077

transferring the secure data to the second computer (See Page 10, Section 0078)

and transferring the secure data from the second computer to the user without using the first computer (See Page 10, Section 0078)

Regarding claim 13, Baird III, et al. discloses the claimed limitation wherein the request to access the secure data includes a strong password and the steps of:

encrypting the secure data with an encryption key (See Page 10, Section 0077)

combining the encryption key with the strong password (See Page 10, Section 0078)

encrypting the combined encryption key and the strong password with a further encryption key (See Page 7, Section 0059).

and transferring the encrypted combined encryption key and strong password and the encrypted secure data to the second computer (See Page 8, Section 0060)

Regarding claim 15, Baird III, et al. discloses the claimed limitation wherein the steps of:

separating the one-time password and the biometric information (See Page 9, Section 0075)

comparing the one-time password to a calculated one-time password (See Page 9, Section 0075)

determining a probability that the biometric information matches an authorized user (See Page 9, Section 0076)

and authorizing access to the secure data only if the one time password matches the calculated one-time password and the probability that the biometric information matches an authorized user exceeds a predetermined threshold value (See Page 10, Section 0077)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 14 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baird III, et al. in view of Epstein (Pub No. 2002/0124176). Regarding claim 14, Baird III, et al. discloses the invention substantially as claimed (See Claim 12), however,

Baird III, et al. does not explicitly teach encrypting the combined password and strong password using an asymmetric encryption key.

Epstein discloses the claimed limitation wherein the step of encrypting the combined password and strong password with an asymmetric encryption key (See Page 4, Section 0033). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Baird III, et al.'s authentication method with Epstein's biometric mechanism, implementing secure communication within a network device.

Regarding claims 21-22, Baird III, et al. discloses the invention substantially as claimed (See Claim 1), however, Baird III, et al. does not explicitly teach concatenating the biometric data with a one-time password nor using one or more arithmetic operations.

Epstein discloses the claimed limitation wherein concatenating the biometric data with the one-time password to form the strong password (See Page 3, Section 0026)

Epstein discloses the claimed limitation wherein combining the biometric data with the one-time password using one or more arithmetic operations with a result used as the strong password (See Page 4, Section 0031)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Baird III, et al.'s authentication method with Epstein's biometric mechanism, implementing secure communication within a network device.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
December 19, 2005

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137